Privacy

Poullet, Yves

Published in:
Telebanking, teleshopping and the law

Publication date:
1988

Document Version
Publisher's PDF, also known as Version of record

Chapter 7.
Privacy

Telebanking and teleshopping services raise special problems with regard to the protection of data concerning individuals. This chapter is limited to the consideration of these special problems. The focus will be upon the following areas:

1. the particular dangers posed by telebanking and teleshopping services;
2. the parties involved in these transactions and their interests; and
3. the regulations adopted in this area and their evaluation.

7.1. Particular dangers posed by these transactions

Apart from the dangers common to the use of any telematic service, telebanking and teleshopping services present certain specific dangers. For instance, the use of any telematic service allows one to know the precise times when the user is at home, etc. Telebanking and teleshopping services allow additional inferences which may be cause for concern such as consumer habits and, in the case of telebanking services, the total amount and the composition of the user's portfolio and the way in which it is managed. Knowledge of the location of automatic terminals and point-at-sale terminals allows the monitoring of the movements of consumers.

The American O.T.A. (Selected EFT Issues: Privacy, Security and Equity, 1982, p. 29) notes:

> 'With increased use of EFT there will be a large number of points at which traditional norms of privacy could be invaded. More EFT terminals will be on line, making electronic surveillance a more credible possibility. Single statement reporting of all kinds of financial transactions will become common; more data will be aggregated and thus easier to access. At the same time, there could be broader and swifter dissemination of inaccurate data. Even if customer correction of data is facilitated, it will be more difficult for corrections to catch up with and replace faulty information.'

These particular dangers are easily explained in light of (A) the kinds of data connected with the performance of telebanking and teleshopping services, and (B) their places of processing or storage.

A. Kinds of data

The various kinds of data may be distinguished according to whether they were provided prior to the delivery of the card or even the personal identification number which gives the user access to the service or whether they were generated by the use of the service.

Certain data on individuals are requested at the time when the personal identification number (PIN) is delivered. This type of number is usually necessary in connection with teleshopping and telebanking services which require prior personal identification. Generally, this information is provided in the questionnaire which is completed before the signature of the subscriber's contract.

This data on individuals, which is gathered at the time the personal identifications code is requested, identifies the account and concerns the profession, age, name and other characteristics of the subscriber. The collection, processing and storage of this information are covered by general provisions on privacy and raise few problems. In contrast, the data generated by the use of the service are more varied and give rise to certain problems.

A distinction may be drawn between data generated by the use of the service and data generated by the performance of the transaction.

This first category of data may be divided into the following sub-categories:

- data linked to the transmission of the message, that is, information necessary to permit the communication of the message: this data poses few problems.
- data linked to the management of the service such as the account number, the personal identification number, etc.
- data linked to the content of the message and the transaction performed.

It should be noted that these data concern primarily the user; however, in the case of certain services, the data may concern third parties (e.g. the identification of the beneficiary of the payment in the case of electronic fund transfers and, particularly, point-of-sale services).

The second category of data principally concerns facts related to billing in the case of teleshopping services. These facts do not pertain to third parties, but only to the users themselves.

B. Places of processing or storage

The report on privacy drawn up in conjunction with the topic 'Electronic Press' (report made for the D.G. XIII, not published) emphasized that the channels used by the service for the transmission of data on individuals are characterized by a lack of transparency. From a theoretical standpoint, this lack of transparency is due to the large number of participants involved in a teleshopping or telebanking transaction. In addition to the parties involved in the basic transaction, there may be companies concerned with the technical aspects of the service, a clearing house, and the beneficiary's bank. In the case of point-of-sale transactions, processing or storage of information may be performed by branches or integrated in a centre shared by the various branches or even different companies.

Finally, the information obtained from the user or generated by the use of the service may be stored in various locations. These may be borrowed from international networks by using those portions of the network which are temporarily idle (changes may be caused by rate fluctuations or by problems of overloading experienced by certain parts of the network).

7.2. The parties to these transactions and their interests

The performance of a transaction involves 4 parties having different interests:

1. the supplier of the service (the bank in the case of telebanking or the seller in the case of teleshopping)
2. the user of the service (the holder of the personal identification number)
3. in the case of POS, the store where the telebanking terminal is installed;
4. the third party beneficiary who, at times, may be involved in a telebanking transaction.

For the sake of completeness, it should also be noted that certain government agencies involved in the application of tax laws as well as courts concerned with civil or criminal cases may have an interest in gaining access to the information generated by the use of these services.

A. Suppliers of the service

The supplier of the service has three major reasons for wanting to store information on customers. First, he needs the most complete accounting system possible, that is, one which records each transaction. Such a system is necessary to ensure the completion of the transaction (e.g. payment, delivery of products). The record of the transaction gives the supplier evidence of the transaction intiated by the user, evidence which also fulfils the statutory accounting requirements of each country. It should be noted that the strictness of this evidentiary requirement may vary according to the purpose it is designed to fulfil. For the purpose of recording the transaction for the user, the record should be as complete as possible. On the other hand, the information recorded for accounting or tax purposes does not need to be so complete. Finally, information on customers which is generated by the use of teleshopping and telebanking services gives the supplier of the service an excellent knowledge of his clientele – their identity, location and preferences in the case of individuals and the supplier's market in the case of banks, which may be particularly important when their are a number of retailers using point-of-sale terminals. This information is useful for the purposes of marketing as well as for the evaluation of the credit of users and retailers (size of their market, fluctuations in demand, etc.)

B. User of the service

1. Advantages

For the user, the processing and storage of data generated by the use of the service entails certain advantages. From a technical standpoint, the continuity of the service is ensured since the user may take up the communication where it was left off in the event that the communication is interrupted. Also, the fact that the user receives a copy of the information stored by the supplier helps him manage his budget as well as to document the transactions for the purposes of tax declarations (e.g. monthly purchases of gasoline). Finally, the user is able to require the seller to produce evidence concerning the transaction in the event of litigation.

2. Disadvantages

The treatment and storage of data also entails certain disadvantages for the user:

- The user's ability to obtain credit may be impaired if certain information is kept on file too long (e.g. information showing that the user has repeatedly overdrawn his account). Also, the user's credit rating may be downgraded if the rating system automatically excludes consumers who have certain habits or make certain kinds of purchases. Finally, the user may be blacklisted and, thus, prevented from using the service a all.
- The anonymity of the user may also be threatened, which may cause concern in the case of someone who makes an anonymous charitable contribution through an electronic payment system.
- Individual freedoms may be affected such as the freedom of expression (e.g. subscription to a particular publication) or the freedom of movement (e.g. monitoring of the user's movements).

C. Seller

Apart from the fact that a credit card is often viewed as guaranteeing payment, the installation of a point-of-sale terminal by the seller serves several purposes. First, it facilitates the management of the seller's accounting records. Second, it provides the seller with valuable marketing information such as the preferences of each customer. Finally, it provides evidence of the transaction in the event of litigation.

D. Beneficiaries

For various reasons, the third party beneficiary may be concerned with ensuring that the automatic processing of data connected with telebanking services

does not allow the supplier of the services to obtain information on him such as the source of his income. This concern is shared by the numerous third parties inevitably involved in the transaction.

E. Governmental Authorities

In connection with the enforcement of tax laws, it is likely that the authorities may be interested in gaining access to information generated by the use of telematic services, particularly in so far as it would allow them to monitor the transactions carried out by both retailers and consumers. In this connection, it should be noted that this was the reason that in 1984 French law added the electronic payment card to the list of means of payment which the retail store must accept.

F. Courts

For the courts, the information generated by the use of telematic services may serve two purposes: (1) it may prove the existence of a transaction which is challenged; and (2) it may prove that a person was at a specific place at a specific time, information which may be important in a criminal proceeding.

7.3. Regulations in the field

A distinction may be drawn between principles derived from general legislation on privacy and privacy in banking on the one hand, and specific regulations adopted in the field of telebanking and teleshopping on the other.

A. Principles derived from general legislation on privacy

The convention adopted by the Council of Europe the 28th of January 1981 constitutes a common standard for the various member countries. The adoption of such a standard at a pan-European level, adoption recommended by the European Community, and its incorporation in the national legislation of each member country (this is not always the case for Belgium, Italy, Portugal and the Netherlands) allows the advancement of a common market in teleshopping and telebanking services where individual privacy is protected.

The following comments may be made with respect to the application of such a standard to these services:

- the principle of *relevancy* or "purposes limitation" laid down in this resolution and incorporated in national legislation, particularly that of West Germany and Denmark, requires the supplier of teleshopping and

telebanking services to clearly identify the purpose for which the information is gathered, the kind of information required for the completion of each type of transaction and the length of time the data must be kept on file (e.g. the preservation of data beyond the time when the account is opened, an example provided by France's National Credit Council, Rapport sur les aspects juridiques des nouveaux moyens de paiement, July 1986).

It would seem that such a flexible and gradual application of the principle of relevancy is preferable to the *a priori* regulation of data banks based on the kind of data which is processed or to a system which requires prior authorization. The adoption of the principle of relevancy allows a sectoral approach which forces institutions to clearly identify the final purpose for which they need the data on individuals.

The recording and storage of data concerning individuals generated by teleshopping services are activities which may be justified as serving the following purposes:

a. the performance and, in particular, the billing for telematic services;
b. the need for preserving data in the case of claims by the user;
c. the performance of market studies.

With regard to the limitations placed on the use of the data, the principle of relevancy allows:

a. a limitation to be placed on the rights of the supplier of the service with regard to the collection of preliminary information prior to the supply of the service (e.g. prior to the delivery of an access code).
b. the identification of the kind of data which is processed. In this connection, it should be noted that groups engaged in making sales through telematic services may be required to justify the need to preserve each kind of data (which varies according to the type of service offered), the period for which the data is stored and the employees who have access to the data.

Likewise, according to the American OTA report (cited *supra*, p. 2):

'in payment systems, privacy is violated when data are, without the subject's consent, made available to and used by those not a party to the transaction, for purposes other than those necessary to accomplish the transaction. Those other purposes could range from organized market campaigns to government surveillance to blackmail. If a person has neither explicitly nor implicitly consented to a disclosure and use of information for a given purpose, personal privacy is considered to have been violated even if the same information was willingly provided by that person, either to another party or to the same party for a different purpose.'

- West German and Danish legislations distinguish between enterprises which use data in the context of their own activities and those which process data for others; in the case of the latter, there is stricter regulation of the companies which provide technical services, clearing houses and commercial carriers participating in the transaction without being parties to it.
- It should be noted that, following the establishment of the CNIL, French law prohibits any decision which involves an *evaluation of human behaviour* solely based on 'the automatic processing of information producing a description of the profile or personality of the subject.' This provision applies to credit establishments as well as to businesses using the information generated by the use of the service in order to identify their clientele.
- The principle of adequate '*means of security*' covers the entire data communication network including the access card. In particular, since this involves a card with memory capacity, the supplier of the service must take every possible precaution to ensure that only authorized persons may have access to the information stored in the card's memory. With regard to data transmission, the use of certain security codes may be required in the case of some transactions.

In light of the fact that this field involves an important public interest, legal restrictions must be based on direct or indirect regulation (agreement, licence). This latter approach, which is more flexible and takes greater account of the evolution of technology, is taken up in the framework of a proposed draft concerning the official approval of data processing services offered by the providers of telematic services which is based on security systems developed by them.

B. The principle of secrecy banking

This principle is recognized in both civil law systems and common law systems. In the common law jurisdictions, there is the well-known rule laid down by the court in *Tournier v. National Provincial and Union Bank of England* ([1924] 1 K.B., 461):

'It is an implied term of a contract between a bank and customer that the Bank will not disclose to third persons, without the consent of the customer's account, or any of his transactions with the Bank, or any information relating to the customer acquired through the keeping of his account, unless the Bank is compelled to do so by order of a court, or the circumstances give rise to a public duty of disclosure, or the protection of the bank's own interests requires it.'

In civil law, apart from the implicit contractual obligation (BGH, 4 March 1973), professional or banking secrecy is also protected by criminal sanctions. This secrecy concerns confidential disclosures such as the amount held in the account and specific transactions, but it does not cover more general information such as that pertaining to the customer's solvency. It is not clear whether this obligation covers disclosures made to other bankers who are bound by the same obligation of professional secrecy.

Finally, there are derogations from the obligation of secrecy in all the civil law jurisdictions:

1. The banker may not invoke the obligation of professional secrecy to avoid testifying in a civil or criminal proceeding.
2. In the event that the assets in the customer's account are the subject of an attachment proceeding, the banker may not invoke the obligation of professional secrecy in an effort to protect those assets.
3. If a court needs to evaluate the financial situation of a debtor in order to rule on the individual claims of creditors, the oligation of professional secrecy may not be invoked by the banker.
4. The right to information of the tax authorities has priority over the obligation of professional secrecy.

C. Specific regulations

The specific dangers posed by telebanking and teleshopping transactions (*see supra*) have created a need for specific regulations. The content and implications of these regulations are examined below.

1. Content

- *The simplified standards adopted by the French CNIL concerning the management of bank accounts and credit contracts.* It should be noted that the CNIL was obliged to modify its original position that the data should be subject to a rule of nondisclosure. In fact, it was found necessary to allow banks to distribute among themselves blacklists concerning loss, theft or excessive withdrawals while, at the same time, the principle that data may only be kept on record for a given period was refined further.
- *Article 9 of the Bildschirmtextstaatvertrag* applicable to teleshopping and telebanking services was examined in the report already quoted and entitled 'Electronic Information Services and Privacy'. This article limits the use of data as well as the period of time during which it may be preserved.

Article 9(3) of the Staatsvertrag provides that the Bundespost (which functions as both a transporter and supplier of the service) may only process data necessary for the billing for communication services, that is, data which concerns the duration, the type and the amount involved in the transaction. This article also provides that data necessary for billing purposes may not be used for creating statistical profiles of clients by the Bundespost and limits the period for which the data may be preserved to that necessary for the collection of payment. Paragraph 6(2) of the same article also prohibits the creation of a statistical profile by suppliers of the service without the consent of the user. Enterprises responsible for the performance of the service are bound by these same obligations of secrecy.

The approach adopted by the Bildschirmstextvertrag offers several insights concerning teleshopping:

- in this field, it is important that all of the suppliers of the service in Europe operate in a similar fashion;
- these common practices should be based on flexible norms developed in collaboration with the users and applied under the supervision of the institutions created by legislation on privacy;
- users shoud be informed of these practices regardless of whether they enter into contracts with the suppliers of the services (some services are not based on such contracts) as well as when they acquire the means of access to these services (e.g. the acquisition of a terminal). Users should be supplied with information, free of charge, concerning the supplier's obligation to protect their privacy.
- these standards should specify the kinds of uses which are authorized. In this connection, it is interesting to note how legislation on privacy has evolved. Earlier legislation focused on so-called 'sensitive' data. More recent legislation, such as the Bildschirmtextvertrag, regulates the various categories of users, thus allowing restrictions to be placed on the use of data generated by users in the context of mail-order shopping.

The *1978 Danish Act on Payment Cards* is also noteworthy. Certain articles apply the general principles developed in the area of privacy legislation. Certain information must be given in writing to the firms and individuals at the time when an application is made for a payment card including personal data which the card holder must disclose. This law also regulates the use and disclosure of such personal data as well as the various transactions which may be performed. Finally, this law sets forth the procedures to be followed that a card is lost or stolen and is used by unauthorized persons.

Articles 24 *et. al.* are even more important:

'24(1). Only information on card holders necessary for the carrying out of payment transactions and information on instances where a payment card has disappeared or been revoked due to misuse may be registered.
(2) Information on card holders may only be used and, disclosed when necessary for the carrying out of payment transactions, corrections or legal enforcement, or when authorized by legislation. Information on misuse may only be disclosed to the extent necessary to avoid further misuse.
(3) Information on payment creditors may only be used and disclosed when necessary for the carrying out of payment transactions, corrections and legal enforcement. Information may otherwise only be disclosed to the extent authorized by other legislation.
25. Information on the use of payment systems by individuals and businesses is filed for five years whereupon it is destroyed. However, information on misuse shall be destroyed two years after the registration at the latest.
26. Having obtained the opinion of the Data Surveillance Board, the Minister

of Industry shall make regulations directing that information relative to persons domiciled in this country may only be registered and processed in this country.'

The *Right to Financial Privacy Act* was adopted in the United States in 1978 in response to the recommendations of the Privacy Protection Study Commission. It sets forth the circumstances in which the authorities may gain access to information on individuals or closely-held corporations (less than 5 persons). The authorities may only obtain such information on the basis of:

- the written consent of the customer;
- a summon issued by a court or administrative body; or
- search warrant.

This Act also codifies the principle of secrecy in banking discussed above.

The draft of the U.S. 'EFT Privacy Act, which was analyzed in a recent OTA report, contains certain distinctive features. It introduces the notion of an 'EFT Service Provider', that is 'Any person who provides services including data processing, telecommunications and courier services, intended to accomplish or facilitate, during the period between initiation and completion of a transfer, and electronic fund transfer, but only in regard to the operations of the person in the actual provision of services intended to accomplish or facilitate an electronic fund transfer.' This notion thus covers all parties involved in a transaction including the retail store where the terminal is installed. It includes all persons who physically participate in an electronic fund transfer.

The EFT Privacy Act protects physical and legal persons. It prohibits any disclosure of information concerning the existence, time, place, content, and the effect or significance of an EFT, whether to a private individual or a public authority, except in certain well-defined circumstances.

It should be noted that the 1978 EFT Act already required that the customer should be fully informed as to the policy of the financial institution at the time when the contract allowing the use of the EFT system is signed. However, the 1978 Act did not go so far as to require the bank to reveal the precise nature of the information disclosed or to allow these disclosures to be challenged.

2. *Lessons*

This brief survey of specific regulations reveals certain principles:

- the necessity of defining in advance the kinds of uses to which information concerning individuals may be put in connection with the use of the service and the period for which such information may be kept on file as well as the exclusion of certain uses (i.e. the transfer of files to third parties, *see*, art. 9 of the Bildschirmtextstaatsvertrag and the Danish legislation).
- the recognition of an extended right to information for the consumer of telebanking and teleshopping services, particularly when the application for the card is made and when the card is first used.

the recognition of a specific status for third parties involved in the transaction so that they are bound by the same secrecy obligations as the suppliers of the services themselves (e.g. the various banks involved in the payment system, *see* draft EFT Privacy Act and discussion on the norms proposed by the CNIL).

the opportunity which exists in this field to adopt a set of common standards in order to prevent divergent national legislation.